LITE DEPALMA GREENBERG, LLC
Joseph J. DePalma
Bruce D. Greenberg
570 Broad Street, Suite 1201
Newark, New Jersey 07102
(973) 623-3000

(Additional Counsel on the Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: AMERICAN MEDICAL COLLECTION AGENCY, INC. CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: All Actions Against Inform Diagnostics, Inc. a/k/a Inform Diagnostics Life Sciences, Inc.; Aloha Laboratories, Inc.; Catalina Skin Institute, LLC; Lakewood Pathology Associates, Inc. d/b/a Miraca Life Sciences; and Cohen Dermatopathology, P.C., d/b/a Miraca Life Sciences and PLUS Diagnostic (Other Labs Track)	Civil Action No. 19-md-2904 (MCA)(MAH) **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT: INFORM DIAGNOSTICS**

TABLE OF CONTENTS

Plaintiff Pernell Thomas ("Thomas" or "Plaintiff"), individually and on behalf of classes of all those similarly situated (the "Class" or "Class Members"), upon personal knowledge of the facts pertaining to Plaintiff and on information and belief as to all other matters, and upon the investigation conducted by Plaintiff's counsel, brings this class action complaint against Inform Diagnostics, Inc. ("Inform Diagnostics" or "Defendant"),[1] and alleges as follows:

PRELIMINARY STATEMENT

1. In July 2019, Defendant informed patients to whom it provided various healthcare services that an unauthorized user or users accessed the system run by Inform Diagnostics' billing collections vendor, Retrieval-Masters Creditor's Bureau, Inc., d/b/a American Medical Collection Agency ("AMCA"), between August 2018 and March 2019 (the "Data Breach"). After accessing AMCA's systems, the hacker exfiltrated the sensitive personal, financial, and health testing information of millions of Defendant's patients and sold the information for profit on underground websites known as the "dark web."

2. Plaintiff brings this class action because Defendant failed in its basic, legally bound, and expressly-promised obligation to secure and safeguard its patients' protected health information ("PHI") and personally identifiable information ("PII")—such as Plaintiff's and Class Members' names, mailing addresses, phone numbers, dates of birth, Social Security numbers, information related to Plaintiff's and Class Members' medical providers and services (such as dates of service and referring doctor) and other private information—such as credit and debit card numbers, bank account information, insurance, and insurance subscriber identification number (all collectively referred to as "Personal Information").

[1] As additional facts come to light, Plaintiff may respectfully seek leave to amend this Complaint in order to bring additional causes of action by plaintiffs from other states.

3. As of today, approximately 173,617 Inform Diagnostics patients have had their Personal Information compromised as a result of the Data Breach. As a result of Defendant's failure to protect the consumer information it was entrusted—and legally obligated—to safeguard, Plaintiff and Class Members suffered a loss of value of their Personal Information and have been exposed to and/or are at imminent and significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. In fact, some Class Members' identities have already likely been stolen.

4. Defendant could have prevented this theft had it limited the customer information it shared with business associates and employed reasonable measures to assure its business associates implemented and maintained adequate data security measures and protocols in order to secure and protect customers' data.

5. Defendant's intentional, willful, reckless, and/or negligent conduct—including failing to prevent the Data Breach, failing to limit its severity, failing to detect it in a timely fashion, and failing to timely notify Plaintiff and the Class—damaged Class Members uniformly. As discussed herein, fraudulent activities have already been linked to Defendant's conduct. For this reason, Defendant should pay for appropriate identity-theft protection services and reimburse Plaintiff and the Class for the costs caused by Defendant's sub-standard security practices and failure to timely disclose the same. Plaintiff and the Class are, therefore, entitled to injunctive and other equitable relief that safeguards their information, requires Defendant to significantly improve its security, and provides independent, expert oversight of Defendant's security systems.

JURISDICTION AND VENUE

6. This Consolidated Amended Complaint is intended to serve as an administrative summary as to all other complaints consolidated in this multidistrict litigation asserting claims

against Inform Diagnostics and shall serve for all purposes as an administrative device to aid efficiency and economy for the Class defined below. As set forth herein, this Court has general jurisdiction over Defendant and original jurisdiction over Plaintiff's claims.

7. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 putative Class Members, and minimal diversity exists as Defendant and at least one Class Member are citizens of different states.

8. This Court has personal jurisdiction over Defendant because it maintains sufficient minimum contacts in New Jersey such that it intentionally avails itself of this Court's jurisdiction by conducting operations here and contracting with companies in this District. Additionally, the United States Panel on Multidistrict Litigation transferred all related matters to this District, so Plaintiff is bringing his claims against Defendant in this litigation before this Court.

9. Venue is proper in this District pursuant to 28 U.S.C. § 1407 and the July 31, 2019 Transfer Order of the Judicial Panel on Multidistrict Litigation in MDL 2904 or, in the alternative, pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this District. Venue is also proper because Defendant transacts business and may be found in this District.

NAMED PLAINTIFF

10. Plaintiff Pernell Thomas ("Thomas" or "Plaintiff") is a citizen and resident of the state of North Carolina.

11. Upon information and belief, Plaintiff Thomas visited medical providers in North Carolina who sent his laboratory work and Personal Information to Inform Diagnostics.

12. Upon information and belief, Plaintiff Thomas' bill from Inform Diagnostics was

subsequently sent to Defendant's billing-collections vendor, AMCA.

13. On July 22, 2019, Plaintiff Thomas received a notice of the data breach at AMCA in connection with Inform Diagnostics, stating that his Personal Information may have been compromised.

14. As an Inform Diagnostics patient, Plaintiff Thomas believed that Inform Diagnostics would protect his Personal Information once he provided it to Defendant or its vendors.

15. Plaintiff Thomas would not have provided Inform Diagnostics with this Personal Information nor used Inform Diagnostics had he known that it would fail to protect his Personal Information.

16. Plaintiff Thomas spent time and effort investigating the Data Breach and monitoring his checking and savings accounts to detect fraudulent activity. Plaintiff Thomas suffered and will continue to suffer damages due to the Data Breach, including additional time and effort investigating the Data Breach, monitoring his checking and savings accounts to detect fraudulent activity, and the threat of future, additional harm including, without limitation, credit-card theft, identify theft, false-tax-return information submitted, a false loan submitted, expenses for credit monitoring, expenses for lifting credit-security freezes, and reduced credit scores.

DEFENDANT INFORM DIAGNOSTICS

17. Defendant Inform Diagnostics, Inc. is incorporated in the State of Texas and is a pathology laboratory services company with its headquarters at 6655 North MacArthur Avenue in Irving, Texas.

FACTUAL ALLEGATIONS

A. The Data Breach Impacted Patients of a Wide Variety of Healthcare Organizations, Including Inform Diagnostics

18. Between August 1, 2018 and March 30, 2019, an unauthorized user or users gained access to the AMCA system that contained information obtained from various entities, including Inform Diagnostics, as well as information that AMCA collected itself.

19. Approximately 173,617 Inform Diagnostics patients have been affected by the Data Breach, making it one of the largest health-related data breaches reported to the U.S. Department of Health and Human Services ("HHS") in 2019.[2] The overall AMCA Data Breach (including all impacted laboratories) was the second largest to be reported since HHS's Office for Civil Rights launched its breach portal in 2010.[3]

20. On February 28, 2019, Gemini Advisory identified a large number of compromised payment cards while monitoring dark-web marketplaces where payment card data, and associated PII, is bought and sold. Almost 15% of these records of compromised payment cards included additional PII, such as dates of birth, Social Security numbers, and physical addresses. A thorough analysis indicated that the information was likely stolen from the unsecure online portal of AMCA. Several financial institutions also collaboratively confirmed the connection between the

---

[2] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Jan. 9, 2020); *see also August 2019 Healthcare Data Breach Report*, HIPAA Journal, https://www.hipaajournal.com/august-2019-healthcare-data-breach-report/ (last visited Jan. 9, 2020).

[3] *July-reported healthcare breaches exposed 22 million people's data*, Modern Healthcare, https://www.modernhealthcare.com/cybersecurity/july-reported-healthcare-breaches-exposed-22-million-peoples-data (last visited Oct. 9, 2019).

compromised payment card data and the breach at AMCA.[4]

21. "On March 1, 2019, Gemini Advisory attempted to notify AMCA," but as Gemini Advisory reportedly told DataBreaches.net, "they did not get any response to phone messages they left." Failing to obtain any response from AMCA, Gemini Advisory "promptly contacted federal law enforcement, which reportedly followed up by contacting AMCA."[5]

22. Following notification from law enforcement, AMCA's payment portal became unavailable for weeks.[6]

23. In a written statement attributed to AMCA in June, it announced it was still investigating the breach:

> We are investigating a data incident involving an unauthorized user accessing the American Medical Collection Agency system," reads a written statement attributed to the AMCA. "Upon receiving information from a security compliance firm that works with credit card companies of a possible security compromise, we conducted an internal review, and then took down our web payments page.
> . . . .
> We hired a third-party external forensics firm to investigate any potential security breach in our systems, migrated our web payments portal services to a third-party vendor, and retained additional experts to advise on, and implement, steps to increase our systems' security. We have also advised law enforcement of this incident. We remain committed to our system's security, data privacy, and the protection of personal information.[7]

---

4 *American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory*, DataBreaches.net (May 10, 2019), *available at* https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/.

5 *Id.*

6 *Id.*

7 *LabCorp: 7.7 Million Consumers Hit in Collections Firm Breach, Krebs on Security* (June 4, 2019), https://krebsonsecurity.com/2019/06/labcorp-7-7m-consumers-hit-in-collections-firm-breach/; *see also Information about the AMCA Data Security Incident*, LabCorp, https://www.labcorp.com/AMCA-data-security-incident (last updated June 10, 2019).

B. Inform Diagnostics' Patient Information Was Exposed By The Data Breach

1. Inform Diagnostics Obtained Personal Information Of Plaintiff And Class Members And Shared That Information With AMCA

24. Inform Diagnostics provides anatomic pathology laboratory services to providers throughout the country, including subspecialty diagnostic services in dermatopathology, gastrointestinal pathology, hematopathology, breast pathology, urologic pathology, and neuropathology.[8] It claims to provide "the most reliable, high-quality anatomic pathology laboratory services in the market."[9] Upon information and belief, Inform Diagnostics a/k/a Inform Diagnostics Life Sciences, Inc., Aloha Laboratories, Inc., Catalina Skin Institute, LLC, Lakewood Pathology Associates, Inc. d/b/a Miraca Life Sciences, and Cohen Dermatopathology, P.C., d/b/a Miraca Life Sciences[10] and PLUS Diagnostics,[11] maintains laboratories in Alabama, Arizona, California, Connecticut, Hawaii, Maryland, Massachusetts, Michigan, New Jersey, New York, Ohio, and Texas.[12]

25. Upon information and belief, Inform Diagnostics charges patients for the services it provides to them and its invoices include only fees for such services. Patients are responsible for paying Inform Diagnostics for performing services either through their insurance or out-of-pocket, if the patient does not have insurance or the costs are not entirely covered by insurance.

26. If Inform Diagnostics' patients fail to pay their invoices within the requested time

---

8 https://www.informdx.com/About-Us.aspx (last accessed Jan. 9, 2020).

9 https://www.informdx.com/Our-Services.aspx (last accessed Jan. 9, 2020).

10 https://www.informdx.com/Privacy-Practices.aspx (last accessed Jan. 15, 2020).

11 https://www.businesswire.com/news/home/20080721005181/en/Lakewood-Pathology-Associates-Announces-New (last accessed Jan. 15, 2020).

12 https://www.informdx.com/About-Us/Laboratory-Certifications.aspx; https://www.njportal.com/DOR/BusinessNameSearch/Search/BusinessName (last accessed Jan. 15, 2020).

period, Inform Diagnostics employs an associated business for collection. During the relevant time period, based upon information and belief, Inform Diagnostics utilized AMCA as a billing collection agency.

27. Upon information and belief, in order to facilitate collection, Inform Diagnostics provided AMCA with its patients' Personal Information, which AMCA in turn stored in its own computer systems. In addition, as part of AMCA's billing collection services for Inform Diagnostics, Plaintiff furnished Personal Information directly to AMCA, which AMCA subsequently stored.

2. Inform Diagnostics Informs Patients That They Were Impacted by the Data Breach

28. Inform Diagnostics began informing its patients in or around July 2019 that AMCA had been subject to a data privacy incident and that the breach may have included their PII and PHI including name, identity of medical providers, and dates of service.

29. Inform Diagnostics also informed its patients that the AMCA breach, which compromised their PII and PHI, occurred between August 1, 2018 and March 30, 2019.

30. On July 11, 2019, Inform Diagnostics advised the OCR of the Data Breach and that 173,617 individuals were impacted. OCR is currently investigating the matter.[13]

31. Inform Diagnostics failed to provide proper, timely notice of the Data Breach sufficient to allow its patients to take steps to protect themselves.

32. Despite the fact that AMCA was notified of the data breach on March 20, 2019, Inform Diagnostics did not notify its patients until July 2019.[14]

---

[13] *Cases Currently Under Investigation*, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[14] Inform Diagnostics Statement Regarding AMCA Data Breach (July 26, 2019), https://www.businesswire.com/news/home/20190726005402/en/Inform-Diagnostics-Statement-

3. Inform Diagnostics Committed to Safeguarding its Patients' Personal Information

33. Inform Diagnostics agreed that it was bound to the privacy and security policies of the health care plans concerning its patients and that its Privacy Policy supplemented each health care plan policy pursuant to Inform Diagnostics' Customer Agreements with those health care plans.

34. Inform Diagnostics' Privacy Policy—available via its website—applies to all information collected by its website, mobile applications, and online services that operate and link to the Privacy Policy (such as a patient portal, allowing individuals to pay their bills online). Inform Diagnostics' Notice of Privacy Practices, indicates that it is "committed to protecting medical information" and acknowledges the "obligations [it has] regarding the use and disclosure of [patients'] medical information. Inform Diagnostics also acknowledges being required by Federal Law to "maintain the privacy of [patients'] medical information and take reasonable steps to protect medical information that identifies [patients] from unauthorized disclosure"[15]

35. Inform Diagnostics thus provided patients with a false sense of security that, by using its website, patients would have a secure way of providing their PII and PHI to Inform Diagnostics.

C. Defendant Failed to Exercise Due Care

36. Defendant failed to exercise due care in protecting patients' information by contracting with AMCA to handle debt collections.

37. AMCA's bankruptcy filings indicate how thinly capitalized the company was and

AMCA-Data-Breach

[15] Inform Diagnostics Notice of Privacy Practices, https://www.informdx.com/Privacy-Practices.aspx (last accessed Jan. 9, 2020).

how insignificant its information technology ("IT") department and infrastructure were. Public reporting has suggested that AMCA is not a reputable business associate—let alone an associate to be trusted with Class Members' Personal Information.

38. Specifically, AMCA's bankruptcy filings admit that it had less than $4 million in liquidity and its owner had to take a secured loan from his own personal money simply to mail notices to those impacted by the Data Breach. Put simply, Defendant should not have contracted with an entity that did not even have the means to mail notices to people without having to file for bankruptcy.

39. The length of time between the breach and AMCA's claimed discovery of the breach indicates that AMCA's systems to detect intrusion, detect unusual activity, and log and report such events were woefully inadequate and not in compliance with industry standards. For example, according to technology-security company FireEye, the median amount of time between when a data breach occurs and when it is detected was 78 days in 2018. This number has consistently been on a downward trend in recent years due to improvements in detection computer technology.[16] The fact that it took AMCA 242 days to detect the Data Breach, nearly 3.5 times the median time for detection in 2018, is direct evidence of its failure to employ reasonable, industry-standard data security practices to safeguard Plaintiff's and Class Members' Personal Information. AMCA's data security deficiencies would have been apparent had Inform Diagnostics adequately investigated.

40. AMCA's inability to detect its own Data Breach, when an unrelated security firm (Gemini Advisory, which was not working for AMCA) was apparently able to do so with ease, is

---

16 *M-Trends 2019: FireEye Mandiant Services Special Report, available at* https://content.fireeye.com/m-trends (last visited June 11, 2019).

further evidence of the fact that AMCA employed inadequate data-security practices, and that Defendant failed in its independent obligations to ensure that its HIPAA business associate employed reasonable and industry-standard data security measures. The FireEye report indicates that in 2018, the median amount of time that it took a third-party (like Gemini Advisory) to detect a data breach was three times the median time for internal detection.[17]

41. One of the easiest ways to minimize exposure to a data breach is to limit the type and amount of information provided to third-party business associates and routine destruction or archiving of inactive PII and PHI so that it cannot not be accessed through online channels. Access to millions of patient records through AMCA's online portal should not have been possible, had AMCA maintained appropriate protections. The sheer number of records suggests that AMCA was not destroying or archiving inactive records. Again, Defendant would have discovered this had it exercised adequate oversight over its business associates and audited the data security protocols utilized by AMCA.

42. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). AMCA was not encrypting payment card information according to minimum industry standards of PCI DSS.

43. The payment card industry has published a guide on point-to-point encryption and its benefits in securing payment card data: "point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive

17 *Id.*

authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[18]

44. Defendant had an obligation to exercise oversight over AMCA in a manner that would include immediate knowledge of any data security incidents experienced by AMCA that could affect Defendant's patients. For example, AMCA pointed to the fact that it learned of the unauthorized access in March 2019 through a series of CPP notices suggesting that a "disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges." However, Defendant did not learn of the unauthorized access until months later in May 2019.

45. Defendant agreed, and had continuing contractual and common-law duties and obligations, to keep confidential the Personal Information its patients disclosed to it and to protect this information from unauthorized disclosure. Defendant's agreements, duties, and obligations are based on: (1) HIPAA; (2) industry standards; (3) the agreements and promises made to Plaintiff and Class Members; and (4) Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §45. Class Members provided their Personal Information to Defendant with the reasonable belief that Defendant and its business associates would comply with their agreements and any legal requirements to keep that Personal Information confidential and secure from unauthorized disclosure.

46. HIPAA requires that Defendant provide every patient it treats, including Plaintiff and Class Members, with a privacy notice.

47. As described herein, Defendant's privacy notices informed Plaintiff and Class

---

[18] *Securing Account Data with the PCI Point –to-Point Encryption Standard v2*, available at https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf (last accessed June 11, 2019).

Members that the Defendant would safeguard and protect PII and PHI, and that Defendant could only use or share PHI for specific purposes.

48. As alleged above, AMCA was a "business associate" of Defendant with whom Defendant shared Personal Information of its patients. As Defendant's business associate, AMCA was required to maintain the privacy and security of Plaintiff's and Class Members' Personal Information. HIPAA mandates that a covered entity (*i.e.*, Defendant) may only disclose PHI to a "business associate" (*i.e.*, AMCA) if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[19] Defendant failed to ensure that its business associate, AMCA, safeguarded Personal Information of Defendant's patients and that AMCA complied with HIPAA's privacy mandates.

D. Defendant Violated HIPAA's Requirements to Safeguard Data

49. Defendant had non-delegable duties to ensure that all information it collected and stored was secure, and that any associated entities with whom it shared member information maintained adequate and commercially-reasonable data security practices to ensure the protection of plan members' Personal Information.

50. Defendant is covered by HIPAA (*see* 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[19] *See* 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e).

51. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

52. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

53. HIPAA requires that Defendant implement appropriate safeguards for this information.

54. HIPAA further mandates that covered entities such as Defendant may disclose PHI to a "business associate," such as AMCA, *only* if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[20]

55. HIPAA requires that Defendant provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—*i.e.* non-encrypted data.

56. Despite these requirements, Defendant failed to comply with its duties under HIPAA and its own Privacy Practices. Indeed, Defendant failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protect Plaintiff's and the Class Members' Personal

[20] *See* 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e).

Information;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Take safeguards to ensure that Defendant's business associates adequately protect protected health information;

i. Ensure compliance with the electronically protected health information security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Train all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected

health information, in violation of 45 C.F.R. § 164.530(b).

57. Defendant failed to comply with its duties under HIPAA and its own privacy policies despite being aware of the risks associated with unauthorized access of members' Personal Information.

E. Defendant Was on Notice That Highly Valuable Personal Information of its Patients Could Be Breached

58. Defendant was, or should have been, aware that it was collecting highly valuable data, for which Defendant knew, or should have known, there is an upward trend in data breaches in recent years.[21] Accordingly, Defendant was on notice of the harms that could ensue if it failed to protect patients' data.

59. HHS' Office for Civil Rights currently lists 550 breaches affecting 500 or more individuals in the past 24 months.[22]

60. As early as 2014, the FBI alerted the healthcare industry that they were an increasingly preferred target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (PII)" so that these companies can take the necessary precautions to thwart such attacks.[23]

---

21 *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited January 14, 2020) ("Our healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published.").

22 *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited January 15, 2020).

23 Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited Sept. 27, 2019).

61. The co-founder of Lastline, a network security provider, said that "Hackers target financial companies, like this billing collection company, as they often store sensitive financial information that can be turned into immediate gains."[24]

62. At the end of 2018, the healthcare sector ranked second highest in the number of data breaches among measured sectors, and had the highest rate of exposure for each breach.[25] With this Data Breach, 2019 has seen the exposure of three times the number of records compromised in 2018.[26]

63. Other experts have stated that the Data Breach is at "the intersection of three of the types of data that hackers most desire: personal identifying information that can be used for identity fraud, information about medical conditions, and financial account information."[27]

64. This same article asked: "why did a collections agency have all of this information in the first place?" It also questioned why medical information and Social Security Numbers needed to be provided to debt collectors.[28]

65. Further, Cathy Allen, CEO of Shared Assessments, a cyber-risk management group, stated that "just the types of test proscribed might indicate a type of illness that you would

---

[24] Christopher Rowland, *Quest Diagnostics discloses breach of patient records*, WASH. POST, June 3, 2019, https://www.washingtonpost.com/business/economy/quest-diagnostics-discloses-breach-of-patient-records/2019/06/03/aa37b556-860a-11e9-a870-b9c411dc4312_story.html?utm_term=.78dd30c03a88 (last visited Sept. 27, 2019).

[25] *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center, https://www.idtheftcenter.org/2018-data-breaches (last visited Apr. 21, 2019).

[26] *Healthcare Data Breach Statistics* (August 2019), HIPPAA Journal, https://www.hipaajournal.com/august-2019-healthcare-data-breach-report (last visited Sept. 27, 2019).

[27] Scott Ikeda, *Third Party Data Breach Hits Quest Diagnostics with 12 Million Confidential Patient Records Exposed*, CPO Magazine, June 11, 2019, https://www.cpomagazine.com/cyber-security/third-party-data-breach-hits-quest-diagnostics-with-12-million-confidential-patient-records-exposed/ (last visited Oct. 7, 2019).

[28] *Id.*

not want employers or insurance companies to have. Thieves often steal and resell insurance data on the internet . . . having other information makes the data more valuable and the price higher."[29]

66. Personal Information is a valuable commodity to identity thieves. Compromised Personal Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers and other Personal Information directly on various dark web[30] sites making the information publicly available.[31]

67. Further, medical databases are particularly high value targets for identity thieves. According to one report, a stolen medical identity has a $50 street value on the black market, whereas a Social Security number sells for only $1.[32]

F. Defendant Has Harmed Plaintiff and Class Members by Allowing Anyone to Access Their Information

68. Defendant caused harm to Plaintiff and Class Members by sharing their Personal Information with AMCA without properly monitoring a business associate, and AMCA failed to prevent attackers from accessing and stealing this information in the Data Breach.

---

29 *Id.*

30 The dark web refers to encrypted content online that cannot be found using conventional search engines and can only be accessed through specific browsers and software. MacKenzie Sigalos, *The dark web and how to access it* (Apr. 14, 2018), https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html (last accessed June 17, 2019).

31 *Here's How Much Your Personal Information Is Selling for on the Dark Web,* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 17, 2019); McFarland et al., *The Hidden Data Economy*, at 3, *available at* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last visited June 17, 2019).

32 *Study: Few Aware of Medical Identity Theft Risk*, Claims Journal (June 14, 2012), https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited June 10, 2019).

69. Given the sensitive nature of the Personal Information stolen in the Data Breach—including names, mailing addresses, phone numbers, dates of birth, Social Security numbers, information related to Plaintiff's and Class Members' medical providers and services (such as dates of service, and referring doctor) and other personal information (such as credit and debit card numbers, bank account information, insurance, insurance subscriber identification number), hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future.

70. In fact, many victims of the Data Breach have likely already experienced harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, medical and healthcare fraud, and unauthorized access to their bank accounts. Plaintiff and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

71. The Personal Information exposed in the Data Breach is highly coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web"—and information tied to this Data Breach has already been offered for sale. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and

healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest. Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail, extortion, and other negative effects.

72. Medical data is particularly valuable to hackers. In June 2016, a hacker reportedly was offering to sell hacked medical records of nearly 700,000 patients for hundreds of thousands of dollars on a "deep web marketplace." [33] Later, the same hacker revealed that he had a database of 9.3 million records from a U.S. insurer that was for sale. [34]

73. In a data breach implicating a medical provider or medical information, consumers face the additional risk of their Health Savings Accounts ("HSAs") being compromised. HSAs are often tied to specialized debit cards used to make medical-based payments. However, they can also be used for regular purchases (albeit incurring a severe tax penalty). Such information is an "easy target" for criminal actors.[35]

74. Fraudulent charges have already been linked to Defendant's billing collector's data handling. Another lab impacted by the Data Breach publicly revealed the exposure of patients' Personal Information only after "a disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges."[36]

---

33 Healthcare under Attack: What Happens to Stolen Medical Records?, June 30, 2016, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/healthcare-under-attack-stolen-medical-records (last visited Sept. 27, 2019).

34 Lording it over the healthcare sector: health insurer database with 9.3M entries up for sale, https://www.databreaches.net/lording-it-over-the-healthcare-sector-health-insurer-database-with-9-3m-entries-up-for-sale/, (last visited Sept. 27, 2019).

35 *Id.*

36 Declaration of Russell H. Fuchs Pursuant to Local Bankruptcy Rule 1007-2 and in Support of "First Day" Motions, *In re Retrieval-Masters Creditors Bureau, Inc.*, No. 19-23185-RDD (Bankr. S.D.N.Y. June 17, 2019), ECF No. 2 at 5-6.

75. In addition, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[37] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

76. As explained further by the FTC, medical identity theft can have other serious consequences:

> Medical ID thieves may use your identity to get treatment—even surgery—or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[38]

77. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[39]

78. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer economic loss and other actual harm

---

37 *The Aftermath 2017*, Identity Theft Resource Center, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Aug. 9, 2019).

38 *Medical ID Theft: Health Information for Older People*, Federal Trade Commission, *available at* https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people (last visited Oct. 7, 2019).

39 *See Study: Medical identity theft is costly for victims,* CNET (Mar. 3, 2010), *available at* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Oct. 11, 2019).

for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their Personal Information;

b. identity theft and fraud resulting from the theft of their Personal Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

h. the continued imminent and certainly impending injury flowing from

potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

79. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[40]

80. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[41]

81. Plaintiff and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[42]

---

[40] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Aug. 9, 2019).

[41] U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (2007), *available at* http://www.gao.gov/new.items/d07737.pdf.

[42] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last

82. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Defendant would have no reason to tout its data security efforts to their actual and potential customers.

83. Consequently, had consumers known the truth about Defendant's data security practices—that it did not adequately protect and store their Personal Information—they would not have entrusted their Personal Information to Inform Diagnostics.

84. Reactions to the Data Breach reflect the severity and breadth of the adverse impact on the American public.

85. The Attorney General of Maryland issued a "Consumer Alert" on June 12, 2019, stating, "Massive data breaches like the one experienced by the AMCA are extremely alarming, especially considering the likelihood that personal, financial, and medical information may now be in the hands of thieves and scammers," said Attorney General Frosh. "I strongly urge consumers to take steps to ensure that their information and personal identity is protected."[43]

86. Connecticut Attorney General William Tong, announcing that Illinois and Connecticut's Attorneys General have opened an investigation into the Data Breach, stated:

> The last thing patients should have to worry about is whether their personal information has been compromised by the entities responsible for protecting it. I am committed to ensuring that impacted patients receive timely notification and that the companies involved take precautions to protect consumers' sensitive health and financial information in the future.[44]

---

visited Aug. 9, 2019).

[43] Brian E. Frosh, Attorney General, Maryland, Consumer Alert (June 12, 2019), http://www.marylandattorneygeneral.gov/press/2019/061219.pdf.

[44] *Connecticut and Illinois Open Investigation into Quest Diagnostics, LabCorp Data Breach*, The Office of Attorney General William Tong, *available at* https://portal.ct.gov/AG/Press-Releases/2019-Press-Releases/CT-AND-IL-OPEN-INVESTIGATION-INTO-QUEST-AND-LABCORP-DATA-BREACH.

87. Other State Attorneys General, including the Attorneys General of Michigan, Minnesota, and North Carolina, have also launched investigations into the Data Breach.[45]

CLASS ACTION ALLEGATIONS
NATIONWIDE CLASSES

88. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> All natural persons residing in the United States whose Personal Information was compromised in the Data Breach**.**

89. The Nationwide Class asserts claims against Defendant for negligence (Count 1), negligence *per se* (Count 2), unjust enrichment (Count 3), declaratory judgment (Count 4), and breach of implied contract (Count 5).

STATEWIDE SUBCLASS

90. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of North Carolina claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes, on behalf of a separate North Carolina subclass (the "Statewide Subclass"), defined as follows:

> All natural persons residing in that North Carolina whose Personal Information was compromised in the Data Breach.

91. The Statewide Subclass asserts claims against Defendant for violations of the North Carolina Unfair Trade Practices Act, N.C. Gen. Stat. §75.1.1, *et seq.* (Count 6), and the North Carolina Identity Protection Act, N.C. Gen. Stat. §§ 75-60, *et seq.* (Count 7).

92. Excluded from the Nationwide Class and the Statewide Subclass are the Defendant,

---

[45] *AMCA Data Breach Tally Passes 20 Million as BioReference Laboratories Added to List of Impacted Entities*, HIPPA Journal, https://www.hipaajournal.com/amca-data-breach-tally-passes-20-million-as-bioreference-laboratories-added-to-list-of-impacted-entities/ (last visited Oct. 9, 2019).

any entity in which the Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and the Statewide Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

93. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**. The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, approximately 173,617 Inform Diagnostics patients had their data compromised in the Data Breach. Those individuals' names and addresses are available from Defendant's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

94. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether Defendant had a duty to protect Personal Information;

b. Whether Defendant failed to take reasonable and prudent security measures;

c. Whether Defendant knew or should have known of the susceptibility of AMCA's systems to a data breach;

d. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Defendant's security measures to protect its systems were reasonable in light of known legal requirements;

f. Whether Defendant was negligent in failing to adequately monitor and audit the data security systems of its vendors and business associates;

g. Whether Defendant's efforts (or lack thereof) to ensure the security of patients' Personal Information provided to business associates were reasonable in light of known legal requirements;

h. Whether Defendant's conduct constituted unfair or deceptive trade practices;

i. Whether Defendant violated state law when it failed to implement reasonable security procedures and practices;

j. Which security procedures and notification procedures Defendant should be required to implement;

k. Whether Defendant has a contractual obligation to use reasonable security measures;

l. Whether Defendant has complied with any contractual obligation to use reasonable security measures;

m. What security measures, if any, must be implemented by Defendant to comply with its contractual obligations;

n. Whether Defendant failed to notify Plaintiff and Class Members as soon as practicable and without delay after the data breach was discovered;

o. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of AMCA's systems and/or the loss of the Personal Information of Plaintiff and Class Members;

p. Whether Plaintiff and Class Members were injured and suffered damages

or other losses because of Defendant's failure to reasonably protect their Personal Information; and,

q. Whether Plaintiff and Class Members are entitled to damages, declaratory relief, or injunctive relief.

95. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class Members. Plaintiff's Personal Information was in Defendant's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to those of other Class Members and Plaintiff seeks relief consistent with the relief of the Class.

96. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

97. **Predominance & Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and

the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendant and, thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

98. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for Defendant or would be dispositive of the interests of members of the proposed Class.

99. **Ascertainability.** The Class and Subclass are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the class. The Class and Subclass consist of individuals who received services from Defendant and whose accounts were placed into collections with AMCA by Defendant. Class Membership can be determined using Defendant's and AMCA's records contained in their databases.

100. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

101. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification

because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendant failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiff and the Class Members;

c. Whether Defendant failed to adequately monitor and audit the data security systems of their vendors and business associates;

d. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

NEGLIGENCE

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

102. Plaintiff repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

103. Defendant required Plaintiff and Class Members to submit Personal Information to obtain diagnostic and medical services, which Defendant provided to AMCA for billing purposes. Defendant collected and stored the Personal Information for commercial gain.

104. Defendant knew or should have known that AMCA's web payments page was vulnerable to unauthorized access by third parties.

105. Defendant had a non-delegable duty to ensure that contractual partners with whom

it shared patient information maintained adequate and commercially-reasonable data security practices to ensure the protection of patients' Personal Information.

106. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class Members' Personal Information within its control from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

107. Defendant owed a duty of care to Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the Personal Information.

108. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and the Plaintiff and Class Members. The special relationship arose because Plaintiff and Class Members entrusted Defendant with their confidential data as part of the health treatment process. Only Defendant was in a position to ensure that its contractual partners had sufficient safeguards to protect against the harm to Plaintiff and Class Members that would result from a data breach.

109. Defendant's duty to use reasonable care in protecting Personal Information arose as a result of the common law and statutes and regulations, as well as its own promises regarding privacy and data security to its patients. This duty exists because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of Plaintiff and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future if Defendant did not protect Plaintiff's and Class Members' information from hackers.

110. Defendant's duties also arose under HIPPA regulations, which, as described above, applied to Defendant and establish national standards for the protection of patient information, including protected health information, which required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The duty also arose under HIPAA's Privacy Rule requirement that Defendant obtain satisfactory assurances from its business associate AMCA that AMCA would appropriately safeguard the protected health information it receives or creates on behalf of the Defendant. 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

111. Defendant's duties also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, several individual states have enacted statutes based upon the FTC Act that also created a duty.

112. Defendant knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its vendors' and business associates' systems, and the importance of adequate security.

113. Defendant breached its common law, statutory, and other duties—and thus were negligent—by failing to use reasonable measures to protect patients' Personal Information, and by failing to provide timely and adequately detailed notice of the Data Breach.

114. Defendant breached its duties to Plaintiff and Class Members in numerous ways,

including, without limitation, by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' Personal Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to adequately monitor and audit the data security systems of its vendors and business associates;

d. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

e. Failing to adequately monitor, evaluate, and ensure the security of AMCA's network and systems;

f. Failing to recognize in a timely manner that Plaintiff's and other Class Members' Personal Information had been compromised; and

g. Failing to timely and adequately disclose that Plaintiff's and Class Members' Personal Information had been improperly acquired or accessed.

115. Plaintiff's and Class Members' Personal Information would not have been compromised but for Defendant's wrongful and negligent breach of their duties.

116. Defendant's failure to take proper security measures to protect sensitive Personal Information of Plaintiff and Class Members caused a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' Personal Information.

117. It was also foreseeable that Defendant's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and other Class Members.

118. Neither Plaintiff nor the other Class Members contributed to the Data Breach and subsequent misuse of their Personal Information as described in this Complaint.

119. As a direct and proximate cause of Defendant's conduct, Plaintiff and the Class suffered damages and will suffer damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Personal Information of Plaintiff and Class Members; damages arising from identity theft or fraud; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take years to discover and detect; and loss of the value of their privacy and confidentiality of the stolen confidential data, including health data.

COUNT 2

NEGLIGENCE PER SE

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

120. Plaintiff repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

121. Defendant is an entity covered by HIPAA (45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

122. HIPAA requires Defendant to "reasonably protect" confidential data from "any

intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). HIPAA also requires Defendant to obtain satisfactory assurances that their business associates would appropriately safeguard the protected health information it receives or creates on behalf of the Defendant. 45 CFR § 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA. AMCA constitutes a "business associate" within the meaning of HIPAA.

123. HIPAA further requires Defendant to disclose the unauthorized access and theft of the Personal Information to Plaintiff and the Class Members "without unreasonable delay" so that Plaintiff and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information. *See* 45 C.F.R. §§ 164.404, 406, 410.

124. Defendant violated HIPAA by failing to reasonably protect Plaintiff's and Class Members' Personal Information, as described herein.

125. Defendant's violations of HIPAA constitute negligence per se.

126. Plaintiff and Class Members are within the class of persons that HIPAA was intended to protect.

127. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

128. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

129. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

130. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information they obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as Defendant, including, specifically, the immense damages that would result to Plaintiff and Class Members.

131. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

132. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

133. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

134. As a direct and proximate result of Defendant's negligence per se under HIPAA and the FTC Act, Plaintiff and the Class have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT 3

UNJUST ENRICHMENT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

135. Plaintiff repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

136. Plaintiff and Class Members have an interest, both equitable and legal, in the

Personal Information about them that was conferred upon, collected by, and maintained by Defendant and which was ultimately stolen in the Data Breach.

137. Defendant received a monetary benefit from Plaintiff and Class Members' conferring their Personal Information, which Defendant retains and uses for business purposes and profit.

138. Plaintiff's and the Class Members' Personal Information was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that Personal Information.

139. But for Defendant's commitment to maintain the confidentiality and security of their Personal Information, Plaintiff and the Class Members would not have provided the information to the Defendant.

140. As a result of the wrongful conduct alleged herein, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members. Among other things, Defendant continues to benefit and profit from the use of Plaintiff's and the Class Members' Personal Information, while its value to Plaintiff and Class Members has been diminished and its exposure has caused Plaintiff and Class Members harm.

141. Under the doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, from Plaintiff and Class Members.

142. Equity and good conscience require restitution by Defendant in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including, specifically, the value to Defendant of the Personal Information that was stolen in the Data Breach and the resulting profits Defendant received and continues to receive from the use of that information.

COUNT 4

DECLARATORY JUDGMENT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

143. Plaintiff repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

144. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Defendant to provide adequate security for the Personal Information it collected from them. As previously alleged, Defendant owes duties of care to Plaintiff and Class Members that require it to adequately secure their Personal Information.

145. Defendant still possesses Personal Information pertaining to Plaintiff and Class Members.

146. Defendant has made no announcement or notification that they have remedied the vulnerabilities in its practices and policies regarding ensuring the data security of patients' Personal Information.

147. Accordingly, Defendant has not satisfied its implied contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendant's lax approach towards data security has become public, the Personal Information in their possession and in their vendors and business associates' possession is more vulnerable than it was prior to announcement of the Data Breach.

148. Actual harm has occurred in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide data security measures to Plaintiff and Class Members, including the fact that Class Members' Personal Information was available for sale on the dark web.

149. Plaintiff, therefore, seeks a declaration that (a) Defendant's existing data security

measures do not comply with its obligations and duties of care; and (b) in order to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Modifying its practices and policies to ensure the business associates to which it provides patients' Personal Information engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering vendors and business associates to promptly correct any problems or issues detected by such third-party security auditors;

b. Modifying its practices and policies to ensure the business associates to which it provides patients' Personal Information engage third-party security auditors and internal personnel to run automated security monitoring;

c. Modifying its practices and policies to ensure the business associates to which it provides patients' Personal Information audit, test, and train security personnel regarding any new or modified procedures;

d. Modifying its practices and policies to ensure the business associates to which it provides patients' Personal Information segment Personal Information by, among other things, creating firewalls and access controls so that if one area of a system is compromised, hackers cannot gain access to other portions of the systems;

e. Modifying its practices and policies to ensure only Personal Information necessary for provision of services is provided to business associates;

f. Modifying its practices and policies to ensure Personal Information not necessary for the provision of services is purged, deleted, and destroyed, and to ensure its

business associates likewise purge, delete, and destroy such Personal Information;

g. Conducting regular security checks of the business associates to which it provides patients' Personal Information;

h. Routinely and continually conduct internal training and education to inform internal security personnel how to monitor the data security of business associates to whom patients' Personal Information is provided; and

i. Educating its patients about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendant's patients must take to protect themselves.

COUNT 5

BREACH OF IMPLIED CONTRACT
On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

150. Plaintiff repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

151. Plaintiff and Class Members were required to provide their Personal Information, including names, addresses, Social Security numbers, financial information, and other personal information, to Defendant in order to complete medical and diagnostic tests.

152. When Plaintiff and Class Members provided their Personal Information to Defendant in exchange for services, they entered into an implied contract with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and adequately notify them if their data had been breached and compromised.

153. Plaintiff and the Class Members would not have provided and entrusted their

Personal Information to Defendant in the absence of the implied contract to keep the information secure.

154. Plaintiff and the Class Members fully performed their obligations under the implied contract with Defendant by providing their Personal Information, whereas Defendant did not comply with its obligations to keep the information secure.

155. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' Personal Information, which was compromised as a result of the Data Breach.

156. As a direct and proximate result of Defendant's breach of their implied contacts with Plaintiff and Class Members, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity as to how their Personal Information is used; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information in their continued possession; and, (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of

Plaintiff and Class Members.

CLAIMS ON BEHALF OF THE STATEWIDE SUBCLASS

157. In the alternative, the claims asserted above are also brought on behalf of a North Carolina subclass.

COUNT 6

NORTH CAROLINA UNFAIR TRADE PRACTICES
On Behalf of Behalf of Plaintiff and the North Carolina Subclass

158. Plaintiff repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

159. This cause of action is brought under North Carolina's Unfair Trade Practice Act, N.C. Gen. Stat. § 75-1.1, *et seq.* (the "NCUTPA").

160. Under the NCUTPA, unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful.

161. At all times material hereto, Defendant committed unfair or deceptive acts or practices in violation of NCUTPA by committing acts or practices that, *inter alia*, offend established public policy, as embodied in North Carolina privacy laws and Section 5 of the FTC Act, and are immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers including, but not limited to, representing that goods or services have characteristics, uses, or benefits that they do not have.

162. Defendant's unfair and deceptive acts or practices possessed the tendency or capacity to mislead, or created the likelihood of deception, of an average, reasonable consumer.

163. Defendant's unfair or deceptive actions proximately caused injury to Plaintiff and the Class.

164. Defendant engaged in unfair or deceptive acts willfully, and has refused to take

responsibility for them.

165. Plaintiff and North Carolina Subclass members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorneys' fees.

COUNT 7

NORTH CAROLINA IDENTITY THEFT PROTECTION ACT, N.C. Gen. Stat. §§ 75-60, et seq. On Behalf of Plaintiff and the North Carolina Subclass

166. Plaintiff repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

167. Defendant is a "business" that owns or licenses computerized data that includes Personal Information as defined by N.C. Gen. Stat. § 75-61(1).

168. Plaintiff and North Carolina Subclass members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

169. Defendant is required to accurately notify Plaintiff and North Carolina Subclass members if they discover a security breach, or receive notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

170. Plaintiff's and North Carolina Subclass members' Personal Information includes Personal Information as covered under N.C. Gen. Stat. § 75-61(10).

171. Because Defendant discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons) of AMCA's data systems involving the Personal Information of Plaintiff and North Carolina Subclass members that Defendant provided to AMCA, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by N.C. Gen.

Stat. § 75-65.

172. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated N.C. Gen. Stat. § 75-65.

173. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

174. As a direct and proximate result of Defendant's violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass members suffered damages, as described above.

175. Plaintiff and North Carolina Subclass members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorneys' fees.

REQUESTS FOR RELIEF

Plaintiff, individually and on behalf of members of the Class and Subclass, as applicable, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is proper class representative; and appoint Plaintiff's Co-Lead and Co-Liaison Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiff and Class and Subclass members compensatory, consequential, and general damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of its unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary

damages, to the extent permitted by law;

6. That Plaintiff be granted the declaratory relief sought herein;

7. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

8. That the Court award pre- and post-judgment interest at the maximum legal rate; and

9. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

LITE DEPALMA GREENBERG, LLC

Dated: April 23, 2020

/s/ Joseph J. DePalma

Joseph J. DePalma
Bruce D. Greenberg
570 Broad Street, Suite 1201
Newark, New Jersey 07102
(973) 623-3000

James E. Cecchi
CARELLA BYRNE CECCHI
OLSTEIN BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700

Lead Counsel for Plaintiffs

James Pizzirusso
Katie R. Beran
HAUSFELD LLP
1700 K Street, NW, Suite 650
Washington, DC 20006
(202) 540-7200

Laurence D. King
Mario M. Choi
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
(415) 772-4700

Amy E. Keller
Adam J. Levitt
DICELLO LEVITT GUTZLER LLC
10 North Dearborn Street, 11th Floor
Chicago, Illinois 60602
(312) 214-7900

Other Labs Track Co-Lead Counsel

Joseph P. Guglielmo
SCOTT+SCOTT ATTORNEYS AT LAW, LLP
The Helmsley Building
230 Park Ave, 17th Floor
New York, New York 10169
(212) 223-6444

Other Labs Track Steering Committee

Andrew J. Schwaba
SCHWABA LAW FIRM, PLLC
212 South Tryon Street
Suite 1725
Charlotte, North Carolina 28281
Telephone: (704) 370-0220

Edward H. Nicholson, Jr.
NICHOLSON LAW FIRM, P.A.
212 South Tryon Street, Suite 1725
Charlotte, NC 28281
(704) 223-2406

Attorneys for Plaintiff Thomas